

企業ウェブサイトの情報開示とIT監査アプローチ

著者	池田 公司
雑誌名	甲南経営研究
巻	41
号	1・2
ページ	161-193
発行年	2000-10
URL	http://doi.org/10.14990/00003948

企業ウェブサイトの情報開示と IT 監査アプローチ

池 田 公 司

I は じ め に

財務会計は、測定および報告 (measurement and reporting) という二つのプロセスから構成される。前者は会計情報 (財務諸表等) の作成プロセスを、また後者は会計情報を投資者等の外部利用者に提供するプロセスを指している。財務会計とコンピュータとの関わりは、先ず測定プロセスから始まり、1950年代から会計データのコンピュータ処理が行われている。これに対して、報告プロセスのコンピュータ化は大きく遅れ、半世紀後の今日になって漸く実用化の目処がついた。その理由としては、外部報告会計の場合、潜在的投資者を含む不特定多数の利用者に対し、同一条件で情報提供を行う必要があるために、インターネットのような公共ネットワークの整備と高性能・低価格 PC の普及を待たねばならなかったことが挙げられる。

1950年代以降の半世紀を振り返ると、この間の情報システム研究は、EDPS (Electronic Data Processing System) から MIS (Management Information System), DSS (Decision Support System), SIS (Strategic Information System) への展開プロセスに示されるように、専ら組織体の内部利用 (経営者・管理者のための情報システム研究) が中心であった。少なくとも理論的には、AAA による1966年報告書 (Committee to Prepare a Statement of Basic Accounting Theory [1966]) にみられるように「会計は本質的には一

企業ウェブサイトの情報開示と IT 監査アプローチ（池田公司）

つの情報システム」であり、かつ「会計情報は外部利用者（external users）にとってより重要」との認識があったものの、当時の情報技術の水準では外部利用者のための情報システム研究は実現不可能であった。しかしながら、本格的 GUI 指向の PC 用 OS である Windows 95/NT が公表された頃から、一般的エンドユーザのためのインターネット利用環境が急速に整備され始め、インターネット上での財務報告が実用化の域に到達した。このことと相まって、米国 SEC の EDGAR システムや我が国大蔵省の EDINET にみられるように、一方では規制当局による強制開示が電子化の方向へ移行すると同時に、他方では個別企業による任意開示の可能性も現実味を帯びてきた。将来的には、インターネット上で提供される各企業の任意開示情報が、より一層拡張されるものと期待されている。

こうしたことから、インターネット財務報告（強制開示および任意開示）に対する信頼性の保証問題が、新たな監査問題として認識されるようになっていく。本稿では、AICPA および CICA のスタディグループによる研究報告書を手がかりとして、ディスクロージャーの電子化に伴う監査アプローチの変化を検討することにしたい。

II 財務会計のためのシステム監査

我が国では、コンピュータベースで運用されている情報システムの監査を、システム監査と称している。このターミノロジーは、狭義においては、通産省の『システム監査基準』（通商産業省機械情報産業局 [1985] [1996]）に則って行う監査を指している。しかしながら、より広義に、財務諸表監査の一環として実施されている会計システムの監査——日本公認会計士協会の定義によるいわゆる EDP システム監査（日本公認会計士協会 [1980] [1994]）——を含めて用いることも多い。

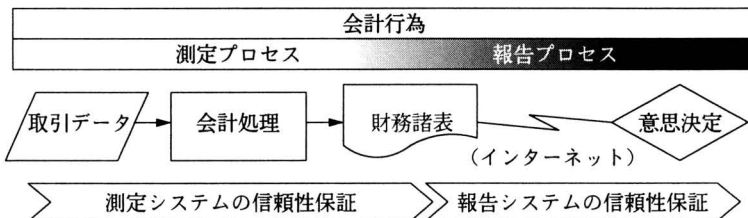
我が国でシステム監査問題が本格的に議論されるようになったのは1980年

代以降のことであり、最近20年間の理解の仕方では、通産省基準のシステム監査がシステム自体の保証であるのに対して、日本公認会計士協会のシステム監査は出力情報（財務諸表）の保証であり、こうした最終的要証命題のウェイトの置き方が両者の違いとされてきた。しかしながら、AICPA のエリオット委員会報告書（Special Committee on Assurance Services [1997]）を契機として、会計的なコンテキストにおけるシステム監査も、システム自体の信頼性保証として考えられるようになり、従来の分類の仕方は、必ずしも妥当しなくなっている。更に、本稿のメインテーマである電子開示の実用化によって、財務報告の在り方も大きなインパクトを受けており、従来のペーパーベースの定期的な開示から、オンラインの継続的な開示へと変化する可能性が指摘されている（Study Group of AICPA/CICA [1999]）。Study Group of AICPA/CICA [1999] では、企業ウェブサイト（corporate Web site）の情報開示に対する信頼性保証手段として継続監査（continuous auditing）が提唱されている。

こうしたドラスティックな会計環境の変化を念頭に置くと、伝統的なシステム監査の概念的整理を見直すことが求められるであろう。本来の意味でのシステム監査のアプローチを、財務会計の測定システムおよび報告システムの両者に適用することが必要になっている。この関係を示したものが「図1」である。

「図1」では次のことを表している。すなわち、財務会計の理論によると、

図1 財務会計の測定・報告とシステム監査



企業ウェブサイトの情報開示と IT 監査アプローチ（池田公司）

会計行為は測定および報告の二つのプロセスから構成される（武田 [1998]）。会計の処理や手続きがペーパーベースであるのか、あるいはコンピュータベースであるのかにかかわらず、この理論的区分は変化するものではない。従って、財務会計の総てのプロセスが電子化された場合においても、その信頼性保証は「図 1」の理論的区分に対応する形で、測定システムおよび報告システムの信頼性保証に分けて考えることができる。

1 測定システム

測定システムの信頼性保証は、最終的な出力情報（歴史的財務諸表を含む会計報告書）のみでなく、測定システム自体の保証を含んでいる。この場合、企業の情報システムにおいて、会計報告書の作成に直接関係のない部分は基本的に保証範囲から外されると考えるのが合理的である。しかしながら、エリオット委員会が提案するように監査上の保証概念を種々な方向に拡張する場合は、監査対象システムも拡張されるであろう。

2 報告システム

報告システムに関しては、強制開示の場合と任意開示の場合に分けて考える必要がある。なぜなら、両者は報告システムの形態を異にするからである。(1)EDGAR や EDINET 等の強制開示の場合では、ファイラー（上場企業）からレギュレーター（大蔵省）への電子ファイリング（electronic filing）の各ステップにおいて、会計情報のインテグリティの保証が問題になる。(2)他方、企業ウェブサイトの任意開示の場合では、先ず、如何なる範囲の情報を如何なるレベルで保証しているかが問題になる。すなわち、他のウェブサイトへのリンクから生じるいわゆる境界問題（boundary problem）と、監査・レビュー・コンピレーションの適用による保証水準の区別を明らかにすることが必要であろう。加えて、電子化された開示に固有な問題として、コンピュータグラフィックスや動画を駆使したマルチメディア指向型の会計プレゼンテーションが、情報利用者に誤解を与えるおそれがないかを検証しなければな

らないであろう。更に、インターネット技術の加速的な発展に伴い、近い将来、企業のデータベースへの直接アクセスが「一定の許可された範囲のデータ」に対して認められるようになり、集約されていない会計データをダウンロードすることや、ウェブサイト上で種々の意思決定支援ツール (what if 分析等) を提供することが行われるようになれば、報告システムの信頼性保証は一層重要な監査テーマになるであろう。こうした任意開示の報告システムや、それに対する信頼性保証が高度化を遂げると、規制当局による強制開示はその存在意義が低減することも予測される。

III IT 監査における三つの理論的方向性

前節では、専ら財務会計のパースペクティブから、システム監査の在り方と対象範囲を検討した。ここでは、通産省基準によるシステム監査や関連する他の問題領域も含めて、システム監査の理論的な方向性を整理し、その中で「財務会計のためのシステム監査」の位置付けを示すことにしたい。とりわけ、米国におけるシステム監査の史的発展プロセスを踏まえつつ、EDP 監査から IT 監査への変化を跡づけ、IT 監査としてのシステム監査には三つの理論的方向性があることを明らかにしたい。

1 EDP 監査としてのシステム監査

監査とコンピュータとの関わりは以外と早く、1950年代におけるコンピュータ会計の実用化と同時に始まっている。AICPA [1983] によると、会計データが初めてコンピュータで処理されたのは1954年のこととされており (AICPA [1983] , p.3), その2年後の1956年に監査法人の Price Waterhouse が *Auditor Encounters Electronic Data Processing* と題する報告書 (Price Waterhouse [1956]) を作成している。このタイトルから理解されるように、当時の会計システムは EDPS と呼ばれ、その監査は EDP auditing と呼ばれた。Price Waterhouse [1956] は、IBM の依頼によってニューヨー

クの Price Waterhouse が内部的に作成したもので、商用コンピュータの導入が内部統制手続や会計記録の監査可能性に及ぼす影響を調査したものである。導入の当初から、IBM のクライアント企業において信頼性の保証問題が発生していた様子がうかがえる。コンピュータの導入に付随する監査問題をクリアしなければ、同社のマーケティング戦略に支障を来したものと付度される。

Price Waterhouse による1956年の報告書から1990年代前半までの発達プロセスを手短に振り返ると、AICPA を中心として EDP 環境における会計情報の信頼性・正確性を保証するための研究努力が蓄積され、全般統制 (general control) と業務処理統制 (application control) によるコントロールの体系や、種々のコンピュータ利用監査技法 (Computer Assisted Auditing Technique; CAAT) が開発されるに至った (AICPA [1968] [1977] [1983] [1990] [1994] [1995]; CICA [1970] [1986] [1998]; COSO [1994]; ISACA [1995])。しかしながら、最初に述べたように、測定プロセスのコンピュータ化に比して、報告プロセスのコンピュータ化が大きく出遅れたことから、専ら前者の監査が中心であった。1980年代にメインフレームを中心とする会計システムから、クライアントサーバシステムへとシステムの処理形態が変化したものの、測定プロセスのみを監査対象とする点では、同じ範疇に属しているといえることができる。

また、この半世紀の間に、情報システムが高度化かつ複雑化したことから、情報システムの監査が一つの独立した監査プロフェッションとして生成されたことも、ここで付言しておく必要がある。米国では1969年に EDPA (EDP Auditors Association) が設立されており、1978年から EDPA によって CISA (Certified Information Systems Auditor) プログラムが実施されている。共通の知識体系が整備され、CISA の職業倫理規定 (code of ethics) も設けられている。我が国では、少し遅れて1980年に日本公認会計士協会の

『EDP システムの内部統制質問書』(日本公認会計士協会 [1980]) が作成されており、1985年に通産省の『システム監査基準』(通商産業省機械情報産業局 [1985]) が策定・公表されている。また、1986年から通産省によってシステム監査の試験制度——情報処理システム監査技術者試験——が開始されている。我が国において、種々のヴァリエーションを含むシステム監査概念が普及し始めたのはこの時期からである。

2 IT 監査としてのシステム監査

1950年代から1990年代前半にかけては EDP 監査 (EDP auditing) が一般的であったが、1990年代後半に入ってから、米国を中心として IT 監査 (IT auditing) が支配的になりつつある。例えば、米国監査法人の Coopers & Lybrand が1998年 (Price Waterhouse との合併前) に公表した外部監査・内部監査のためのシステム監査マニュアルにおいても *Handbook of IT Auditing* (Warren et al.[1998]) というタイトルが用いられているが、この旧版のタイトルは *Handbook of EDP Auditing* であった。IT 監査というターミノロジーにおける IT は「情報技術」(Information Technology; IT) を指しているが、必ずしも厳密な意味での IT の定義が存在しているわけではない。しかしながら、概してインターネットやネットワーク技術をマルチメディアとともに企業の経営戦略や財務戦略に積極的に活用する文脈で用いられているように見受けられ、1990年代の後半からデリバティブとともにビジネスの鍵概念になりつつあることは確かである。

通産省の『システム監査基準』においても、IT を経営戦略に活用することの重要性が認識され、1996年に改訂を受けている (通商産業省機械情報産業局 [1996])。通商産業省機械情報産業局 [1996] においては、CIO (Chief Information Officer) や情報戦略等のターミノロジーの使用が見られるところから、米国企業の動向を踏まえた対応といえよう。通産省の提示した新しい概念枠組みの下では、IT の戦略的利用を企画開発する「システム分析」と、そ

企業ウェブサイトの情報開示と IT 監査アプローチ（池田公司）

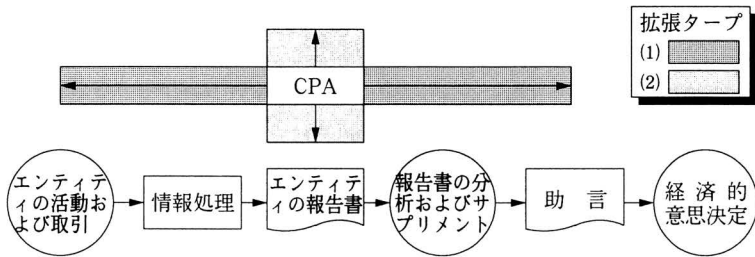
の信頼性・安全性・効率性を保証する「システム監査」が表裏一体のものとして構想されている。併せて、前者の機能の担当主体を対象とした試験制度——システムアナリスト試験——も創設され、この時点で、上記の情報処理システム監査技術者試験はシステム監査技術者試験に名称変更されている。情報戦略は、(1)CEO による経営戦略の立案、(2)その経営戦略に整合した形で CIO による情報戦略の立案、(3)システムアナリストによる情報戦略の実現、および(4)システム監査技術者による情報戦略の信頼性・安全性・効率性の保証という図式になる。通産省基準のシステム監査が、このように内部監査指向的な形で展開してきたことは、我が国通産省がもともと証券市場監督官庁ではなく産業保護官庁としての性格を有することに起因するといえよう。

以上に述べたような最近の動向を整理すると、IT 監査としてのシステム監査には、次の三つの理論的方向性を考えることができる（池田 [1999]）。

- ① 1996年改訂版の『システム監査基準』にみられるように、とりわけ内部監査の立場から、企業の情報戦略（IT strategy）の一環として展開するケース。
- ② 前掲の「エリオット委員会報告書」にみられるように、伝統的財務諸表監査の理論的枠組みを拡張することにより、外部監査の立場からもシステムの信頼性保証（systems reliability assurance）として展開するケース。
- ③ AICPA/CICA の推進している「ウェブトラスト」にみられるように、電子商取引の保証業務（Electronic Commerce Assurance Services; ECAS）として展開するケース（Nagel et al.[1999]）。

財務会計の測定・報告の全プロセスが電子化することに伴う監査問題は、上記②の方向性と関連している。「図2」は Elliott [1994] に基づいて、保証機能を拡張する機会を示したものである。「図2」においては、グレーの網掛けの部分が保証機能の拡張を表しており、(1)監査上の要証命題を情報処理プ

図2 保証機能を拡張する機械



(出所) Elliott [1994], p. 121に加筆修正。

プロセスの上流および下流に向かって拡張するタイプ、および(2)CPA が保証を付与する情報の範囲を拡張するタイプの二つが示されている。既に米国で運用段階に入ったディスクロージャーの電子化や、将来的に想定されるインターネット上での継続的なオンライン財務報告を射程に捉えると、こうした二つ方向での保証機能の拡張が求められる。すなわち、財務会計の測定システムおよび報告システムの信頼性を保証すると共に、とりわけ任意開示のケースにおいては、制度的な規制範囲を超えた会計情報に対しても何らかの信頼性（積極的保証または消極的保証）を付与することが必要であろう。

ところで、上記③の ECAS は、基本的にインターネットショッピングの信頼性保証を意味しており、財務会計が本来的に機軸とする投資意思決定有用性アプローチとは直接的には結び付かない。しかしながら、エリオット委員会の基本的な論調から理解されるように、米国でも監査市場を新規に開拓することが求められており、成長性が見込まれるウェブトラストは監査プロフェッションが参入すべき重要領域と考えられている。AICPA はエリオット委員会の最終報告書を受けて「企業対顧客」(business to consumer) のウェブトラストを開発するとともに、現在「企業対企業」(business to business) のウェブトラストも開発しつつある。前者は専らインターネットショッピングの信頼性保証に終始するが、後者はより拡張された意義を有している。何

企業ウェブサイトの情報開示と IT 監査アプローチ（池田公司）

れにせよ、上記①および②とは異なったコンテキストにおいて、③の方向で展開される領域は今後の重要テーマになるであろう。

なお、自明なことながら、上記②のケースにおける「任意開示」の会計情報と、上記③のケースにおける「企業対顧客」の電子商取引は、同一なウェブサイト上で行われることになる。以下で取り上げる FASB 実験モデルのように、企業ウェブサイトで開示される総ての情報を監査するという考え方も一部には存在するので、上記の②と③は、理論的区分は異なるとしても切り離して論ずることは適切でない。

IV 電子ファイリングシステムの信頼性保証

以下では、前節で識別した IT 監査の三つの方向性のうち「財務会計のための IT 監査」に着目し、ディスクロージャーの電子化に伴う監査アプローチの変化を検討する。既に述べたように、電子開示には、規制当局による強制開示と企業による任意開示の二つの形態が区別され、前者ではファイラーからレギュレーターへの電子ファイリングシステムに関するコントロールの監査（audit of controls over an electronic filing system）が必要になる。すなわち、EDGAR や EDINET では、データベースが規制当局によって管理され、かつ取り扱われる情報内容も制度会計の枠組みで明確に定められているところから、電子ファイリングの各ステップにおいて情報のインテグリティを保証するためのコントロールが設計され、かつ有効に機能しているかを検証することが監査要点となる。本節では先ず強制開示の IT 監査について議論し、次節において任意開示——個別企業によるウェブサイトでの情報開示——の IT 監査を取り上げる。

1 電子ファイリングシステムのリスク

もともと制度会計の報告プロセスを電子化した電子ファイリングシステムは、情報内容のヴァリエーションが少なく、監査要件も伝統的財務諸表監査

の延長上にあるので、監査上の取り組みも相対的に容易であるといえる。Study Group of CICA [1995] によると、電子ファイリングのプロセスは以下の四つから構成され、各プロセスには「表1」に示したリスクが存在する。

- ① ファイラーによる情報作成。
- ② ファイラーによる情報提出、およびレギュレーターによる情報受理と公式承認。
- ③ レギュレーターによる情報分析、利用および蓄積。
- ④ オンラインデータベースまたはインターネット等の公共ネットワークによる一般大衆への情報開示。

2 電子ファイリングシステムのコントロール

また、「表1」の右側の欄に示されるように、個々のリスクに対しては「全般統制」(General Control; GC) および「直接統制」(Direct Control; DC) の二つのレベルでコントロールが検討されており、後者には更に五つのタイプが識別されている。全般統制がその性格上総てのリスクに関係しているのに対して、直接統制は個々のリスクの内容に依存して適用パターンが異なっている。例えば、ファイリングプロセス①を見ると、ソースレコードのフォーマット変換に関するリスクに対しては、全般統制と二つの直接統制 (DC4 および DC5) が挙げられている。なお、「表1」のプロセス②に特徴的に現れているように、電子ファイリングシステムにおいては、ファイラー側のシステムと、レギュレーター側のシステムの二つがリスク評価およびコントロールの対象となる。この点が、次節で取り上げる任意開示のケースと異なっている。

全般統制と直接統制によるコントロールの捉え方は、システム監査で通常用いられている全般統制と業務処理統制の概念枠組みと概ね同義といえよう。しかしながら、具体的なコントロール手続の内容やそれらに対するウェイトの置き方は、電子ファイリングシステムに固有なコンテキストに依存して決

表1 電子ファイリングシステムのリスクおよびコントロール

電子ファイリングシステムにおけるリスクのタイプ	コントロール*					
	DC					GC
	1	2	3	4	5	
① ファイラーの情報作成 ・ ソースレコードをファイリング用フォーマットに変換する際に、正確性や完全性が失われる。 ・ レギュレーターの承認に必要な総ての情報が網羅されていない。 ・ レギュレーターが指摘したファイリングの欠陥が、フォローアップ、修正および再提出されていない。				○	○	○
② ファイラーの提出とレギュレーターの受理・承認 ・ 非権限者が情報を提出する。 ・ 不正確または不完全な情報を提出する。 ・ 送信中に情報の正確性や完全性が失われる。 ・ 間違った相手に情報を送信する。 ・ ウィルスに感染した情報を送信する。 ・ 未承認者からのファイリングを受理する。 ・ 不正確または不完全な情報を受理する。 ・ 受理した旨を適時に通知しない。 ・ 受理した保留中の情報が失われたり改変される。 ・ ファイリングの欠陥を適時に通知しない。 ・ 受理前にウィルスを検知できない。	○	○	○	○	○	○
③ レギュレーターによる分析・利用・蓄積 ・ プログラムエラーで不正確な処理や蓄積が行われる。 ・ オペレータミスで不正確な処理や蓄積が行われる。 ・ データやプログラムが未承認で変更、追加または削除される。 ・ ウィルスに感染または発見できない。 ・ ハードウェアまたはソフトウェア障害によりデータが部分的または完全に喪失する。 ・ データやプログラムが未承認で利用される。	○	○				○
④ 一般大衆への開示 ・ 外部利用者によりデータやプログラムが未承認で変更、追加または削除される。 ・ 公共的にアクセス可能なデータベースに機密情報が含まれる。 ・ 公共的にアクセス可能なデータベースに公表許可前の情報が含まれる。 ・ ウィルスに感染する。	○	○	○			○

注* GC：全般統制（General Control）

DC：直接統制（Direct Control）

DC1：アクセスコントロール

DC2：エディット／ヴァリデーションコントロール

DC3：データ通信コントロール

DC4：照査合計および連番検査

DC5：サスペンスレコードおよび誤謬・例外報告書

（出所）Stuby Group of CICA [1995], pp. 11-12に加筆・修正。

定される。すなわち、この場合、全般統制は次の五つのカテゴリーから構成される (Study Group of CICA [1995], pp.20-24)。

- ① 組織および経営のコントロール。
- ② オペレーティングシステムおよびアプリケーションシステムの開発と保守に関するコントロール。
- ③ コンピュータの操作に関するコントロール。
- ④ データ入力とプログラムに関するコントロール。
- ⑤ セキュリティ、バックアップおよびリカバリーに関するコントロール。

他方、直接統制は、ファイラーによる情報作成からレギュレータによる情報公開まで、電子ファイリングシステムの情報処理に直接影響を及ぼすコントロールを指している。これには、プログラム化されたコントロール手続とユーザによるコントロール手続が含まれる (Study Group of CICA [1995], pp.10-16)。

3 電子ファイリングシステムに関するコントロールの監査

レギュレータやユーザは電子ファイリングシステムが適切に運用されているという保証を必要としているので、コントロールの有効性監査を要求するであろう。この監査には次のような事項が含まれる (Study Group of CICA [1995], p. 31)。

- ① システムの内部統制目的と、その目的達成のために設計されたコントロールに関する記述を通読する。
- ② それらのコントロールがシステムの内部統制目的の達成に十分かつ適当であるかを評価することで、コントロール設計の適切性を評定する。
- ③ 立会・質問およびシステム上のデータ処理を追跡することにより、ある時点におけるコントロールの実在を検証する。または、監査手続の実施により、ある期間を通してコントロールが有効に運用されていることを決定する。

- ④ レギュレーター側のコントロール目的と、その目的達成のために設計されたコントロールは完全かつ正確なものであり、年度を通してコントロールが有効に運用されている旨の陳述書をレギュレーター管理者から入手する。

加えて、電子ファイリングシステムの監査において特に考慮すべき点がある。以下に示すような考慮事項が挙げられる（Study Group of CICA [1995], p. 32）。

- ① 伝統的な紙片形態の監査証拠を利用できない可能性が高い。コントロール機能に関する証拠のほとんどはコンピュータで読み出し可能な形式のみで存在し、しかも短期間しか利用できない場合がある。
- ② コントロールの設計と運用に関する第一義的な責任はレギュレーターにあるが、一部の責任はファイラーにもある。例えば、機密性を有する ID コードを適切に管理することや、正しいバージョンの情報を送信することは、ファイラーの責任である。このように多数のファイラーにも責任の一端があるコントロールについては、有効な運用を保証するのは難しい場合がある。また、多数の外部利用者が電子ファイリングシステムにアクセスすることになるので、システム、プログラムおよびデータに対して未承認アクセスの行われるリスクが高まるであろう。
- ③ 電子ファイリングシステムでは情報通信が最も重要な部分である。従って、情報通信のコントロールを評価する際には、ハードウェア構成要素（例えば、モデム、通信制御装置、通信回線等）の適切性や、メッセージ送受信形式を定義する通信プロトコルに関する専門知識が必要になる。
- ④ 情報技術は急速な発展を続けるものであり、それと同時にデータやプログラムへの不正アクセスを試みる者も増加するので、監査人は常に最新のセキュリティ問題に関心を持たなければならない。

V 企業ウェブサイトの情報開示と信頼性保証

1 インターネットによるビジネスレポーティング

IT とインターネット技術の加速的な発展を念頭に置くと、電子開示システムの今後の展開としては、規制当局による強制開示よりも、個別企業によるウェブサイトでの情報開示がより重要な意義を有すると考えられる。こうした認識は、米国の会計基準設定主体や監査プロフェッションにもみられ、例えば2000年1月31日付けで公表された FASB の *Electronic Distribution of Business Reporting Information* (FASB [2000]) では、インターネットを活用したビジネスレポーティングへの変化について、次のように述べられている。もとより、本稿の目的はビジネスレポーティングを詳細に論ずることではないが、こうしたターミノロジーを新たに使用して会計上の報告概念を拡張することは、インターネットの普及・浸透と有機的に結び付いているといえよう。

「ビジネスのやり方が変化し続けており、この変化が続くとすれば、ビジネスレポーティングも根本的に変化することになるであろう。インターネットが人気メディアになってから、企業、政府機関および投資大衆が情報入手し発信する手段がかつてないほど変化している。今日多くの企業が、規模にかかわらず、インターネットウェブサイトを用いて一般大衆に情報を提供している。それらのウェブサイトにおいて、またあるウェブサイトから他へのリンクにおいて、大量の情報をほんの数秒で入手することができる。オーディオ、ビデオおよびグラフィックスを用いた高度なデータ表示方法が、廉価なパソコンやノートパソコンでさえ利用できる。」(FASB [2000], p.1)

ところで、FASB [2000] には、この問題領域に関連した参考文献が収録されており、そこで用いられているキーワードを要約的に示すと「表2」のようになる (FASB [2000], pp. 81-84)。電子開示に係るキーワードとしては、

表 2 電子開示に係るキーワード

① インターネット
Business Reporting on the Internet
Corporate Reporting on the Internet
Financial Reporting on the Internet
<i>Voluntary</i> Financial Reporting on the Internet
② 企業ウェブサイト
Accounting Information at Corporate Web Sites
Financial Information at Corporate Web Sites
Financial Data at Corporate Web Sites
<i>Voluntary</i> Dissemination of Financial Data at Corporate Web Sites

インターネットと並んで「企業ウェブサイト」(corporate Web site)の使用も多く見られることが一つの特徴をなしている。ここで重要な点は、企業ウェブサイトというターミノロジーの使用自体が、規制当局の強制開示とは異なった独自の伝達チャネルの使用を示唆しており、開示の任意性が強調されていることである。「表 2」においてイタリック体で表示しているように、任意 (voluntary) の電子開示であることを明示する事例も少なくない。また、「表 2」においては示していないが、インベスターリレーションズへのインターネット利用 (use of the Internet for investor relations) や、企業ウェブサイトと有価証券の募集 (corporate Web sites and securities offerings) といったフレーズも見られ、この問題領域の潜在的な拡張性が理解される。

FASB [2000] によると、ウェブサイト上での財務報告は急速に増加しており、Fortune 500 の上位100社中93%が何らかの財務情報を掲載している。こうしたことから、ウェブサイトでの情報開示に対する信頼性保証が一層重要となっており、既に幾つかの取り組みが行われている。とりわけ、次の二つを挙げることができる。

- ① FASB の FauxCom 社 Site Map
- ② AICPA/CICA の継続監査

上記①は FASB のウェブサイト (<http://www.rutgers.edu/accounting/raw/fasb/tech/index.html>) で公開されている実験モデルであり、ホームページの先頭に監査報告書を置き、財務諸表に加えて非財務的・非計量的情報も監査対象としている点に特徴がある。すなわち、FASB の実験モデルはウェブサイトで開示される総ての情報を監査するというという考え方に立っており、上で引用した BRRP (Business Reporting Research Project) の報告書も併せて考慮すると、米国における会計基準設定主体の見解として興味深いものがある。しかしながら、こうした積極的アプローチとは逆に、保証範囲を財務諸表のみに明確に限定すべきとする消極的アプローチも根強く存在していることを付言しておく必要があろう。具体的には AARF 等が挙げられる。

何れの考え方を採るにせよ、こうした積極的・消極的の区別は、保証を付与する範囲の問題であって、監査の実質的なメソドロジーに関する議論を伴うものではない。仮に消極的アプローチを採り財務的・計量的情報のみを監査対象として画定する場合においても、ディスクロージャーの電子化に伴い意思決定に対する情報の質として「適時性」が強調されるならば、伝統的財務諸表監査は有効性を低下させることになるであろう。上記②の AICPA/CICA による継続監査は、情報開示の方法自体が今後「継続的」な形に変化することに着目した監査概念であり、インターネット環境においても有効性を維持しうる監査アプローチが企図されている。以下では、この継続監査を中心にして、企業ウェブサイトの情報開示に対する信頼性保証を検討することにした。

2 継続監査の概念

継続監査の概念は AICPA/CICA の共同研究プロジェクトによる成果であり、近い将来の実用化に備えた「基礎研究」としての性格を有している。Study Group of AICPA/CICA [1999] の序文における次の記述は、監査を取り巻く

環境変化をよく表しており、エリオット委員会の示した基本的方向性をより具体化したものと評価できる。

「監査プロフェッションは、保証業務の市場で起こっている変化に適応しなければならない。その変化は、情報技術の急速な発展によって、増え続けて止まない利用者に大量の情報がより適時に提供されるようになったことが一因となっている。…（中略）…究極的に、監査プロフェッションは、外部利用者に提供される情報に継続的な保証を与えられるよう努力すべきである。」（Study Group of AICPA/CICA [1999], p. v）

こうした認識に基づいて、Study Group of AICPA/CICA [1999] には、とりわけ次のような検討課題が与えられている。

- ① 電子化されたオンライン報告 (electric on-line reporting) の現状と今後の展開。
- ② 継続的に情報開示が行われる環境 (continuous information environment) では、監査業務の性格、タイミングおよび範囲は、伝統的財務諸表監査とどのように異なるか。
- ③ 上記②の環境で有効な監査を実施するために必要な監査人の知識と技能。
- ④ 上記②の環境で有効な監査を実施するために必要な監査戦略とツール。
- ⑤ 外部の意思決定者に対する継続監査報告書の提供に係る問題。

上記①および②に明確に示されているように Study Group of AICPA/CICA [1999] では、加速的に高度化しつつあるネットワーク環境の下で、伝統的財務諸表監査はどのように変化すべきかを明らかにすることが主要な問題意識をなしている。こうした問題意識の下で開発された継続監査モデルは、任意開示としてのインターネット財務報告や、それが一層発展した形態であるデータベース開示 (database disclosure) に対して継続的に信頼性を付与することを目的としており、本稿のテーマである「財務会計のための IT 監査」

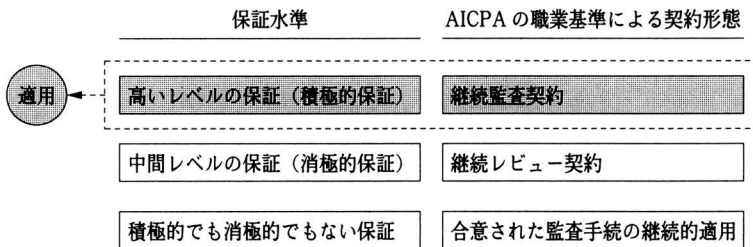
として一つの具体的なビジョンを提示している。

継続監査とは「独立監査人が、監査対象の基礎となる事象の発生と同時に、または短い時間間隔において一連の監査報告書を発行し、監査対象に関する書面による保証を可能にする方法論」(Study Group of AICPA/CICA[1999], p. 5) として定義される。この定義に基づいて、継続監査の性格、目的および範囲 (Study Group of AICPA/CICA [1999], pp. 5-11), および継続監査の実施に必要な条件 (Study Group of AICPA/CICA [1999], pp. 11-18) が識別され、継続監査の概念枠組みが提示されている。

3 継続監査の性格、目的および範囲

上記の定義で示されているように、継続監査の結果は書面による監査報告書として纏められる。従って、継続監査の方法論は AICPA/CICA の職業基準に準拠することが前提となる。「図 3」に示すように、Study Group of AICPA/CICA [1999] では、継続監査においても歴史的財務諸表監査と同様、最も高い水準の保証——積極的保証——を付与することが考えられており、AICPA の SSAE (Statements on Standards for Attestation Engagements) に準拠した「監査」(examination) が実施される。すなわち、レビュー (review) または合意された監査手続 (agreed-upon auditing procedures) を適用して、消極的保証を付与することは予定されていない。監査対象にか

図 3 継続監査の保証水準



(出所) Study Group of AICP/CICA [1999], p. 6に加筆・修正。

かわらず、継続監査は常に積極的保証を付与する契約として理解されている。

ここで、AICPA の SSAE について補足的に説明を加えておきたい。この SSAE は、本稿で取り上げている継続監査に適用されるのみでなく、先に IT 監査の重要な理論的方向性の一つとして識別した ECAS（電子商取引の保証業務）にも適用が義務づけられており、保証機能の拡張と密接に結び付いているからである。

SSAE という名称に用いられている「アテステーション」という概念は、伝統的に、一般に認められた監査基準 (GAAS) に準拠した歴史的財務諸表の監査業務に限定されてきた経緯がある。しかしながら、監査人の提供するサービスが市場の要求に従って拡張した結果、既存の GAAS を適用することはより困難となり、とりわけ財務諸表指向の業務から ECAS 等の新しい業務が引き離される状況が生じてきた。こうしたことから、SSAE の序文では次のように述べられている。

「これらのアテステーション基準および関連する解釈指針を適用する主たる目的は、アテスト機能の一般的な枠組みを提供し、かつ合理的な基礎を設定することにある。そうした趣旨のものとして、基準と解釈指針は、(1)新たに発展しつつあるアテスト業務を実施する公認会計士に有用かつ必要な指針を提供し、また(2)必要に応じて、AICPA の基準設定主体がそのような業務を扱う際の解釈基準を示すものである。」

SSAE は GAAS が自然に拡張したものであり、GAAS と同様に、技術的能力、精神的独立性、正当な注意義務、適切な計画および監督、十分な証拠、および適切な報告の必要性を定めているが、その適用範囲はより広範である。SSAE は、拡張しつつあるアテスト業務に適用され、例えば、内部会計統制システムに関する記述、コンピュータソフトウェアに関する記述、制定法・規制・契約条件への準拠性、投資効率の統計数値、財務諸表の補足情報等に対する契約を含む。このように、SSAE は変化する環境や社会の要求に対処

するために開発されたものである (Nagel et al.[2000])。

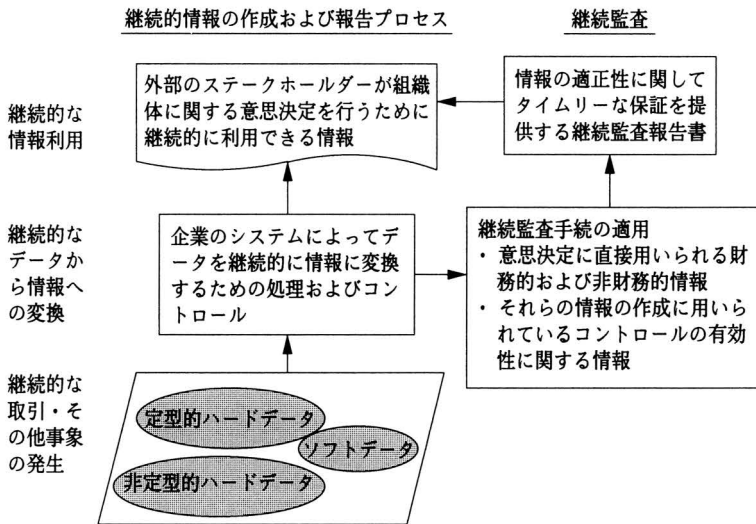
SSAE に準拠して継続監査を実施する際には、「適切な規準」(suitable criteria) を用いて監査対象を評価しなければならない。例えば、財務諸表の継続監査を行う場合においては、一般に認められた会計原則 (GAAP) が適切な規準となる。継続監査では広範な監査対象を取り扱うことになるので、それらの監査対象が目的適合性と信頼性を有する規準に照らして評価されるように考慮しなければならない。

継続監査契約 (continuous audit engagement) における監査人の目的は、監査上の職業判断において「監査対象が適切な規準に準拠していない重要な事実」(a material instance of non-conformity of the subject matter with suitable criteria) を発見できないリスクを十分低いレベルまで下げよう、に、継続監査手続 (continuous audit procedures) の性格、時期および範囲を設計することである。Study Group of AICPA/CICA [1999] では、こうした事実を「誤謬」(error) と定義しており、不正 (fraud) もその中に含まれている。従って、この定義は GAAS における金額的誤謬よりも広範な意義を有している。誤謬の重要性は、監査対象に関する情報に依存しかつ監査対象の基礎となる活動に合理的知識を有するユーザが、意思決定に影響または変更を受ける可能性を考慮して決定される。

継続監査手続の適用から継続監査報告書の作成までの流れを、企業の情報処理プロセスに対応させて示したものが「図4」である。「図4」に示したように、継続監査は(1)経営者の決定したフォーマットで提供される財務的または非財務的な継続情報 (continuous information) に焦点を置くことも、あるいは(2)システムに係るコントロールの有効性に焦点を置くことも可能である。監査人が継続監査報告を依頼される事例としては、次のようなものが挙げられる。

- ① 債務契約への準拠性に関連した特定な財務情報 (例えば、在庫水準、

図4 継続的な情報と監査の流れ



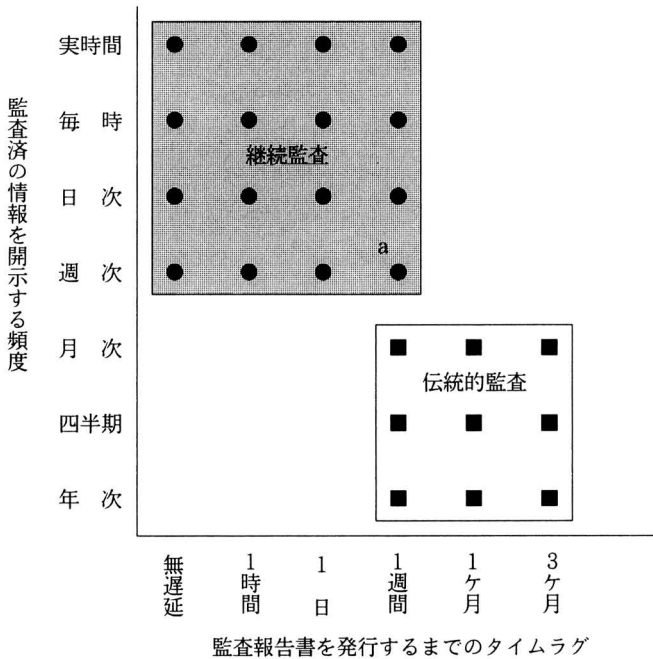
（出所）Study Group of AICPA/CICA [1999], p. 9に加筆・修正。

債権残高、買掛金その他債務の金額および年齢）。

- ② 電子商取引の信頼性、完全性および非拒絶性に関する公表指針・実務への準拠性。
- ③ 公共的にアクセス可能なデータベースにおいて、頻繁に更新される重要情報の完全性および正確性。
- ④ 要求に応じて入手可能な財務諸表。
- ⑤ 公共的にアクセス可能なデータベースのコントロールを含めて、特定のシステムや処理プロセスに関するコントロールの有効性。

とりわけ、上記の例示⑤においては、データベースからダウンロードしたデータを用いることで、ユーザが個人用の情報明細表（information schedule）を作成することが可能となる。システムのコントロールに関する継続監査の目的は、これらのデータの信頼性につきユーザの確信を高めることにあ

図5 継続監査報告書を発行するタイミング



(出所) Study Group of AICPA/CICA [1999], p. 11に加筆・修正。

る。例示①～⑤以外にも、継続監査の対象は種々の業績指標 (performance indicator) に関連付けることができるとされている。

先に示した継続監査の定義によると、「監査対象の基礎となる事象の発生と同時に、または短い時間間隔において一連の監査報告書を発行」するものとされている。「図5」に示したように、継続監査は監査済の情報を開示する頻度と、監査報告書を発行するまでのタイムラグの両面から捉えられている。例えば、開示頻度とタイムラグが共に1週間のシナリオ（「図5」のポイントa）を想定すると、監査人は毎週金曜日の最後に、直前の週の金曜日に作成された情報に関する監査報告を求められることになる。これは週次の報告要

企業ウェブサイトの情報開示と IT 監査アプローチ（池田公司）

件と 1 週間の監査期間を伴う継続監査のパターンである。伝統的な年次財務諸表の監査においても、大規模な被監査会社のケースでは、監査人が年間を通して何らか形で監査業務を継続しているものであるが、これは継続監査とは呼ばない。伝統的財務諸表監査では、監査業務の継続性にもかかわらず、財務諸表と監査報告書は年に 1 度しか作成されないからである。

状況によっては、経営者が監査済の情報をリアルタイムで発行することを希望することも考えられるであろう。そうした状況においては、監査対象の基礎となる事象の発生から、完全な監査対象の入手、監査の実施、および情報とその監査報告書の公表まで、実質的なタイムラグは無い。Study Group of AICPA/CICA [1999] では、こうしたタイプの継続監査によるリアルタイムの監査報告書を、「即時」監査報告書（“immediate” auditor’s report）と呼んでいる。

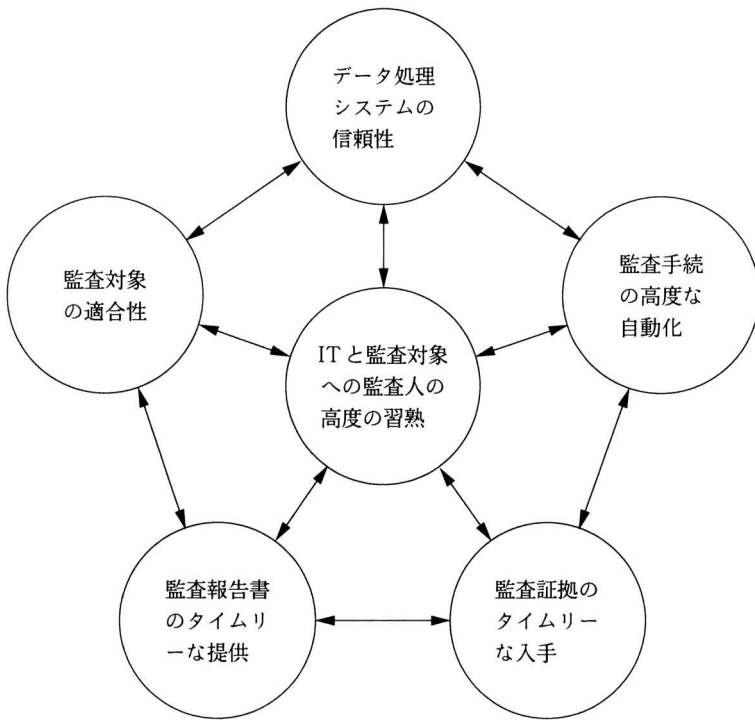
4 継続監査の実施に必要な条件

継続監査の定義によると、監査対象に関連した取引およびその他事象が発生した直後に、監査を実施しかつ報告を行うことが要求される。このような継続監査を可能とするには、相互に関連した諸条件を満たさなければならない。この関係を示したものが「図 6」である。以下、「図 6」の構成要素につき、要点的に説明を加えたい。

先ず監査人は、継続監査契約を締結する前に、監査対象自体の適合性を考慮しなければならない。すなわち、厳しい時間的制約が課せられる継続監査では、監査アプローチ自体を高度に自動化することが求められるので、自動化された監査手続に対する監査対象の適合性を検討することが求められる。

前掲の「図 4」に示したように、情報システムで継続的に処理されるデータには、次の三つのタイプが区別される。この Study Group of AICPA/CICA [1999] による分類は、処理のロジックをプログラム化しうる可能性に基づいている。しばしば、DSS の開発等において、意思決定タイプを定型性

図6 継続監査の実施に必要な条件



(出所) Study Group of AICPA/CICA [1999], p. 12に加筆・修正。

や反復性の観点から類型化する思考法と類似している。経営者および監査人は、継続監査のフィージビリティを検討する際に、タイプ①～③のデータに関連した問題を考慮しなければならない。

- ① 定型的ハードデータ (routine hard data)
- ② 非定型的ハードデータ (nonroutine hard data)
- ③ ソフトデータ (soft data)

タイプ①の定型的ハードデータは、反復的に発生または出現し、かつコンピュータ処理と数値化が容易な事象や条件に関連している。例えば、経営者

が電子商取引の公表方針・実務への準拠性につき継続監査を実施するケースを考えると、監査報告書では、商品が発注された数量と合意された価格で指定された時間内に配達されていることが述べられるであろう。このケースにおける基礎データ（例えば、数量、価格、時間、顧客名と住所）は、明確に定義することが可能でコンピュータ処理も容易である。従って、タイプ①のデータに対する固有リスクと統制リスクは通常低いレベルに押さえられ、経営者による継続報告や監査人による継続監査の可能性が高くなる。

②の非定型的ハードデータは、規則的に発生または出現するものではなく、かつ他のデータと結合しなければコンピュータ処理と数値化ができない事象や条件に関連している。例えば、定期的な実地棚卸から得られる在庫数量、顧客に対する与信限度額の変更、法人税額の計算に必要な税制変更のデータ、受領済・未決済の財貨や役務の発生を確定するためのデータ等が挙げられる。タイプ②のデータは手作業で作成されることが多いので、完全に処理を自動化してコントロールすることは難しくなる。しかしながら、今後システムインテグレーションが推進されると共に、他の情報技術も高度化を続けると考えられるので、従来は非定型的と見なされていたデータも定型的となり、継続報告と継続監査は実施し易くなるであろう。

③のソフトデータは、事象や条件に関して、見積もりを伴う情報を作成する際に適用する仮定や判断に関連している。こうしたデータは主観性が高いため、自動化された処理およびコントロールを行うことは困難である。例えば、銀行は経営者に対して、棚卸資産の正味実現可能価額や銀行借入金の担保にされている諸勘定につき、監査済継続情報を提出するように要求することが考えられる。この場合、信頼しうる正味実現可能価額を算出するには、多くの仮定を設けなければならない。現在では見積もりは人手によって行われているが、情報技術（例えば、ニューラルネットワーク）の発展によって、こうしたプロセスも自動化されるであろう。多くの複雑な仮定に基づいて処

理されるデータは継続監査の実施が一層難しくなるが、タイプ③に対する継続監査の可能性も徐々に高まって行くと考えられる。

監査対象の適合性の次に、継続情報を処理するシステムの信頼性が問題となる。ここに、システムの信頼性 (systems reliability) は「システムが、所与の期間一定条件の下で有効に機能し続ける可能性」として定義される。システムの信頼性は、組織体全体に対するコントロールが有効である場合に最高の水準が達成される。こうしたコントロールは、総論的な意味では COSO [1994] が挙げられるであろう。また、IT のコントロールを有効に設計・運用するための詳細な基準としては、ISACA [1995] や CICA [1998] が挙げられるであろう。

CICA [1998] では、情報技術の戦略計画プロセス (information technology strategic planning process) を展開することが有効なコントロールの達成にきわめて重要であるとされており、そうしたプロセスの要件として次のような事項が挙げられている。

- ① 組織体の諸目的を明らかにしたビジネスモデルと、それらの諸目的に関連した個々の機能や活動。
- ② 組織体の目的達成に必要な情報を入手、処理、蓄積および検索することが保証されるように、実体とデータを識別したデータアーキテクチャー。
- ③ データを獲得、処理および蓄積すると共に、情報を適時、目的適合的および適切な方法で報告するアプリケーションアーキテクチャー。
- ④ 組織体の目的達成に必要なハードウェア、ソフトウェア、通信ネットワークおよびその他設備を構成するテクノロジーアーキテクチャー。
- ⑤ 組織体のニーズの発展に対処するために、現行アーキテクチャーの発展および改善を可能とする移行計画

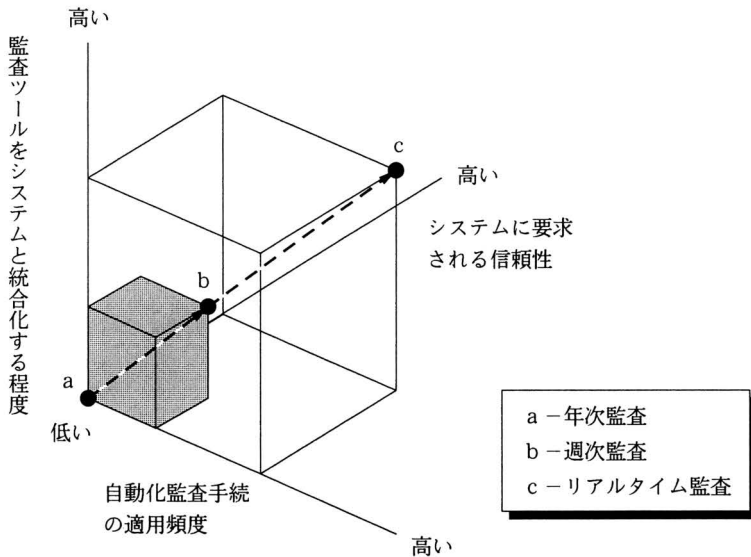
このように CICA [1998] では、システムの企画開発段階から IT の戦略計画を具体化して組み込んでおくことが、運用段階での有効なコントロールに

不可欠であることが強調されている。すなわち、情報戦略に対する経営者のビジョンが不明確な組織体では、競争市場に取り巻かれたシステムのコントロール自体も同様に不明確になるということであろう。この点を考慮すると、通産省基準の IT 監査（内部監査）と財務会計のための IT 監査（外部監査）は接点を有することが理解される。すなわち、『システム監査基準』に則った情報戦略指向的 IT 監査が有効に機能していれば、上記①～⑤の要件はシステムの企画開発段階から保証されていることになり、そのことがシステム運用段階における外部監査のコントロール評価を支援する関係が成立する。外部監査としての継続監査は基本的に運用段階のシステム監査が中心になると考えられるので、こうした内部監査と外部監査の連携が重要になるであろう。

継続監査におけるシステムの信頼性評価とは、システムのコントロールの評価を意味している。すなわち、経営者の導入した全般統制および直接統制が継続的かつ有効に機能しているかを監査人が検証することで、システムの信頼性評価が行われる。全般統制には、組織体における IT 利用全般に係るコントロールが含まれ、具体的には上記の IT 戦略計画を始め、プロジェクト管理、保守管理、セキュリティ対策等が挙げられる。また、内部監査として実施される IT 監査も、ある意味では全般統制の重要な要素を構成するであろう。他方、直接統制は、いわゆる業務処理統制と同義であり、例えばデータ通信やデータベース管理といった個々のアプリケーションや機能に関するコントロールを意味する。

ところで、先に掲げた信頼性の定義によると、システムは「一定条件の下で有効に機能」することが求められている。継続報告および監査のコンテキストにおける一定の条件とは、基礎となる事象や取引が発生した直後に、完全性と正確性を具備した情報を作成しうるシステムの能力を指している。こうした条件を満たすには、高度のシステムインテグレーションと、情報の可用性を中断することなくシステムを改善する能力が経営者に求められる。継

図7 監査報告のタイミングと監査の自動化



(出所) Study Group of AICPA/CICA [1999], p. 17に加筆・修正。

続情報の作成に係る種々のシステムとそれらのサブシステムは、ネットワーク化やデータの共有によって統合化する必要があり、総ての情報構成要素が事実上同時に更新されることを保証しなければならない。現在では、高度なシステムインテグレーションが多く組織体にとって既に可能になっているので、広範な情報の継続報告および監査を行う可能性が高まりつつある。

「図7」は、監査報告のタイミング（年次、週次およびリアルタイム）と、次の三つの変数との関係を示したものである。「図7」に示されるように、監査報告のタイミングが短くなるほど、下記の①～③の各変数に要求される水準が高くなる関係が理解される。

- ① システムに要求される信頼性の程度
- ② 監査ツールをシステムと統合化する程度
- ③ 自動化監査手続の適用頻度

例えば、変数①のシステム信頼性について週次監査（「図 7」のポイント b）と年次監査（「図 7」のポイント a）を比較すると、b の要求水準は a のそれよりも高くなっている。これは、許容される監査期間が短縮されるために、例外や誤謬に対処する時間もそれだけ少なくなるためである。ここに、誤謬が適切な規準からの乖離として定義されるのに対して、例外 (anomaly) とは予定されたデータ形式からの乖離、または予定されたデータ処理またはコントロールからの乖離として定義される。監査対象が適切な規準に準拠している場合であっても、信頼性の低いシステムでは例外処理の発生することがある。継続情報を処理するシステムは、例外や誤謬が頻繁に発生しないように運用されなければならない。

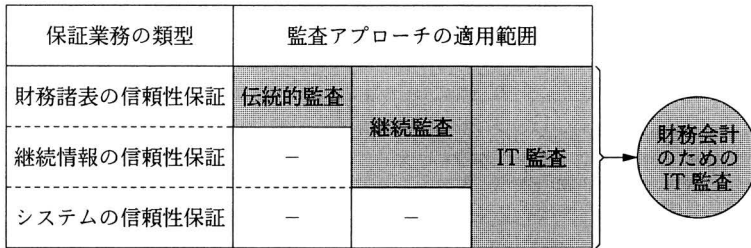
同様に、変数②の監査モジュールの組み込みについても、b では取引データがシステムで処理された直後に監査証拠を収集しなければならないので、a よりも高いレベルが求められることとなる。また、変数③の自動化監査手続の適用頻度では、a のテストが年に 1 度であるのに対して、b のそれはより頻繁なものでなければならない。

究極的に、レベル c の継続監査——即時監査報告書を発行するケース——では、①から③の総てについて最も高度なレベルが要求される。リアルタイム継続監査のフィジビリティを高めるには、企画開発段階における IT 監査を充実させて高信頼性のシステムを構築すること、および企画開発段階から必要な監査モジュールをシステムに組み込んでおくことが求められるであろう。そのためには、内部監査と外部監査の有機的な連携を視野に入れなければならない。

VI 結びに代えて

IT の高度利用が財務会計の報告プロセスに及ぼすインパクトは、(1)企業ウェブサイトでの任意の情報開示が拡張されること、および(2)それのもたらす

図8 ITの高度利用に伴う監査業務の変化



効果として、継続的な情報開示環境の形成が加速されることの二つに集約されると考えられる。「図8」は、この点を踏まえつつ新しい保証業務の類型と、伝統的監査、継続監査およびIT 監査とを対応させて表示したものである。

エリオットによると、保証業務は「情報および／または情報システムの信頼性および／または目的適合性に関する書面または口頭による結論の表明」(the expression of a written or oral conclusion on the reliability and/or relevance of information and/or information systems) として定義される(Elliott [1994], p. 120)。この定義に従うと、外部監査の要証命題にもシステム自体の信頼性保証が包摂され、監査の理論区分としては継続監査よりも一層拡張された内容を有することとなる。「図8」では、エリオットの定義をベースとして「財務会計のためのIT 監査」に対する理論区分を画定している。

【参 考 文 献】

- American Institute of Certified Public Accountants [1968], *Auditing and EDP*, American Institute of Certified Public Accountants. (染谷恭次郎訳 [1970]『会計監査とコンピュータ』日本生産性本部)
- [1977], *The Auditors Study and Evaluation of Internal Control in EDP Systems*, American Institute of Certified Public Accountants.
- [1983], *Auditing and EDP*, Second Edition, American Institute of Certified Public Accountants. (日本公認会計士協会・電子計算機会計委員会訳 [1986]『会計監査とコンピュータ』PMC 出版)

- [1990], *Consideration of the Internal Control Structure in a Financial Statement Audit*, American Institute of Certified Public Accountants.
- [1994], *Auditing with Computers*, American Institute of Certified Public Accountants.
- [1995], *Auditing in Common Computer Environments*, American Institute of Certified Public Accountants.
- Canadian Institute of Chartered Accountants [1970], *Computer Control Guidelines*, Canadian Institute of Chartered Accountants. (平野皓正・高梨智弘共訳 [1979] 『経営・監査のためのコンピュータコントロールの手引き』 日刊工業新聞社)
- [1986], *Computer Control Guidelines*, Second Edition, Canadian Institute of Chartered Accountants.
- [1998], *Information Technology Control Guidelines*, Canadian Institute of Chartered Accountants.
- Committee of Sponsoring Organizations of Treadway Commission [1994], *Internal Control: Integrated Framework*, 2 vols, American Institute of Certified Public Accountants. (鳥羽至英・八田進二・高田敏文共訳 [1996] 『内部統制の統合的枠組み／理論篇・ツール篇』 白桃書房)
- Committee to Prepare a Statement of Basic Accounting Theory [1966], *A Statement of Basic Accounting Theory*, American Accounting Association. (飯野利夫訳 [1980] 『基礎的会計理論』 国元書房)
- Elliott, Robert K. [1994], “Confronting the Future: Choices for the Attest Function,” *Accounting Horizons* (September), pp. 106-124.
- Financial Accounting Standards Board [2000], *Electronic Distribution of Business Reporting Information*, Business Reporting Research Project (BRRP), Financial Accounting Standards Board.
- Information Systems Audit and Control Association [1995], *Control Objectives for Information and Related Technology: COBIT*, Information Systems Audit and Control Foundation.
- Nagel, Karl D., Glen L. Gray [1999], *Electronic Commerce Assurance Services: Electronic Workpapers and Reference Guide*, Harcourt Brace Professional Publishing.
- Price Waterhouse [1956], *Auditor Encounters Electronic Data Processing*, Price-waterhouse. (1998年の Coopers & Lybrand との合併後はニュージャージー州の PricewaterhouseCoopers のライブラリーに保管されている。)
- Special Committee on Assurance Services [1997], *Report of the Special Committee on Assurance Services*, American Institute of Certified Public Accountants (<http://www.aicpa.org/assurance/indx.htm>).
- Study Group of AICPA/CICA [1999], *Continuous Auditing*, Canadian Institute of Chartered Accountants.
- Study Group of CICA [1995], *Electronic Filing of Information: Control and Audit*,

- Canadian Institute of Chartered Accountants.
Study Group of CICA [1999], *The Impact of Technology on Financial and Business Reporting*, Canadian Institute of Chartered Accountants.
Warren, J. Donard, Jr., Lynn W. Edelson, Xenia Ley Parker and Rita M. Thrun (Coopers & Lybrand L.L.P.) [1998], *Handbook of IT Auditing*, 1998 edition, Warren, Gorham & Lamont.
池田公司 [1999]「IT 監査とリスク指向監査アプローチ」會計, 第156巻第4号, 99-113頁。
武田隆二 [1998]『会計学一般教程 (第3版)』中央経済社。
通商産業省機械情報産業局 [1985]『システム監査基準解説書』日本情報処理開発協会。
—— [1996]『システム監査基準解説書』日本情報処理開発協会。
日本会計研究学会スタディグループ [1999]『電子メディアによる情報開示に関する研究／スタディグループ中間報告』日本会計研究学会。
日本公認会計士協会 [1980]『EDP システムの内部統制質問書』日本公認会計士協会。
—— [1994]『情報システムの内部統制』第一法規。